CALIFORNIA HIGH-SPEED RAIL AUTHORITY
DUTY STATEMENT

PARF #46-9-019

CLASSIFICATION TITLE Information Technology Specialist II	**OFFICE/BRANCH** Information Technology	**LOCATION** Sacramento
WORKING TITLE Information Security Analyst	**POSITION NUMBER** 311-001-1414-001	**EFFECTIVE** 02/01/2019

GENERAL STATEMENT:

Under the general supervision of the Information Technology Manager I, the incumbent will work independently as well as part of a team to coordinate and/or perform a variety of Information Technology (IT) services and functions. The incumbent is responsible for performing various oversight duties in support of the California High-Speed Rail Authority's (Authority) Information Security Program ensuring protection of Authority information assets and compliance with federal and state information security mandates, policies, standards, and procedures. The incumbent will also serve as the backup Information Security Officer for the Authority.

This position requires the incumbent to communicate effectively orally as well as in writing; conduct themselves professionally in dealing with other employees and contractors; develop and maintain knowledge and skills related to the position's specific tasks, methodologies, materials, tools, and equipment; complete assignments in a timely and efficient manner, and adhere to departmental policies and procedures regarding attendance, leave, and conduct.

This position is designated under the Conflict of Interest Code. The position is responsible for making, or participating in the making, of governmental decisions that may potentially have a material effect on personal financial interests. The appointee is required to complete form 700 within 30 days of appointment. Failure to comply with the Conflict of Interest Code requirements may void the appointment.

All work will be accomplished in accordance with IT Standards; the State Administrative Manual (SAM) Sections 4800 through 5953 and Sections 6700 through 6780; the California Technology Agency's (CTA) Statewide Information Management Manual (SIMM); the Department of Finance (DOF) Office of Technology Review, Oversight and Security (OTROS) rules and policies; DOF Budget Letters; the State's Information Organization, Usability, Content Currency, and Accessibility (IOUCA) Working Group policies and the Authority's Desktop and Mobile Computing Policy, IT Security policies and procedures and IT Standards.

TYPICAL DUTIES:

Percentage Job Description/Domain
Essential (E)/Marginal (M)

35% (E) **Security Policy, Standards, and Procedures**

Domain - Information Security Engineering

As a member of the Information Security Office, assist with development and maintenance of Authority information security policies and procedures, ensure security roles and responsibilities are identified, coordinated and aligned with internal roles and external partners. Evaluate information security policy needs and develop policies to govern IT activities. Conduct reviews and assessments of IT programs and projects to ensure compliance with plans, policies, standards, and architectures that establish the framework for the IT compliance programs. Analyze processes and procedures to provide recommendations and/or procedural policy changes to improve IT and communication processes. Participate in program, administrative, or operational reviews of Information Security programs to ensure programs and operations are meeting established goals/objectives and regulatory guidelines. Ensure baseline configurations of information technology systems are created and maintained. Ensure all users including; privileged users, third-party stakeholders (e.g., suppliers, customers, partners), senior executives and, physical and information security personnel understand their roles and responsibilities.

35% (E) **Risk Management**

Domain – Information Security Engineering

Ensure Authority compliance with state and federal information security risk management requirements, including State Administrative Manual (SAM) § 5300, et seq., State Information Management Manual (SIMM), and National Institute of Standards and Technology (NIST). Risk management activities include, but are not limited to, identification and prioritization of potential risk assessment projects, maintenance of standards and templates for risk assessments, and compilation of risk assessment data into summary reports. Conduct risk assessments of Information Technology systems and the underlying technical security controls, administrative processes surrounding privacy and security of confidential data, and physical security controls protecting department owned hardware, software, and data. Coordinate and assist with periodic reviews to verify compliance with SAM, SIMM and NIST.

20% (E) **Business Continuity Planning/Technology Recovery Planning**

Domain - Information Security Engineering

Assist with the development, creation and management of an enterprise Business Continuity and Technology Recovery program to ensure timely operations recovery following an interruption in service caused by a technology system outage or a declared disaster. This will encompass the management and/or coordination of the resources required to plan for the restoration of data center operations, recovery of mission-critical business applications and production data, and support of key business continuity objectives. Coordinate business impact analysis and the coordination and management of tabletop and recovery exercises with both business and technical staff.

10% (E) **Marginal Functions**

Domain - Information Security Engineering

Perform other related duties as required to fulfill the Authority's mission, goals and objectives. Additional duties may include, but are not limited to, assisting team/unit staff as needed, which may include special assignments.

KNOWLEDGE AND ABILITIES:

Knowledge of: Emerging technologies and their applications to business processes; business or systems process analysis, design, testing, and implementation techniques; techniques for assessing skills and education needs to support training, planning and development; business continuity and technology recovery principles and processes; principles and practices related to the design and implementation of information technology systems; information technology systems and data auditing; the department's security and risk management policies, requirements, and acceptable level of risk; application and implementation of information systems to meet organizational requirements; project management lifecycle including the State of California project management standards, methodologies, tools, and processes; software quality assurance and quality control principles, methods, tools, and techniques; research and information technology best practice methods and processes to identify current and emerging trends in technology and risk management processes; and state and federal privacy laws, policies, and standards.

Ability to: Recognize and apply technology trends and industry best practices; assess training needs related to the application of technology; interpret audit findings and results; implement information assurance principles and organizational requirements to protect confidentiality, integrity, availability, authenticity, and non-repudiation of information and data; apply principles and methods for planning or managing the implementation, update, or integration of information systems components; apply the principles, methods, techniques, and tools for developing scheduling, coordinating, and managing projects and resources, including integration, scope, time, cost, quality, human resources, communications, and risk and procurement management; monitor and evaluate the effectiveness of the applied change management activities; keep informed on technology trends and industry best practices and recommend appropriate solutions; foster a team environment through leadership and conflict management; effectively negotiate with project stakeholders, suppliers, or sponsors to achieve project objectives; and analyze the effectiveness of the backup and recovery of data, programs, and services.

DESIRABLE QUALIFICATIONS:

- Associates degree required, Bachelor's degree preferred.

ADA Notice: For individuals with sensory disabilities, this document is available in alternate formats. For information, please call the EEO Officer at (916) 324-1541, email at eeo@hsr.ca.gov, or write to: California High-Speed Rail Authority, at 770 L Street, Suite 620, Sacramento, CA 95814.

- 5 years of related experience in Information Security Operations or equivalent combination of education and experience.
- Ability to independently analyze and resolve issues.
- Project lead experience.
- Must have IT-related knowledge demonstrating experience operating or assessing IT components such as data centers, networks, operating systems, infrastructure components, or databases.
- Exercises good judgment in the performance of responsibilities, requiring minimum supervision.
- Exhibits a talent and passion for information security; is creative and resourceful in solving problems.
- Demonstrates the ability to identify organizational IT risk.
- Thorough understanding of NIST, SAM, and SIMM.
- Thorough understanding of the creation of security policies, processes, and procedures in both a commercial and cloud-based network.
- Strong oral and written communication skills.
- Possession of one of the following active certifications:
    - Certified Information Systems Security Professional (CISSP)
    - Certified Information Security Manager (CISM)
    - Certified Information Systems Auditor (CISA)
    - CompTIA Security+
    - GIAC Information Security Fundamentals
    - Microsoft Certified Systems Administrator – Security
    - Associate of (ISC)2

SUPERVISION EXERCISED OVER OTHERS:

This position does not supervise others but may act in a lead capacity. The incumbent will have defined responsibility and authority for decision making related to projects or in an advisory function.

RESPONSIBILITY FOR DECISIONS AND ACTIONS:

At the Information Technology Specialist II level, incumbents are responsible for independent work within business constraints. This level is responsible for the recommendations to executives, decisions for the projects, and outputs. As a subject matter expert, this level is responsible for actions that could have a serious detrimental effect on the operating efficiency of the undertaking or function.

CONSEQUENCE OF ERROR:

The consequence of error at the Information Technology Specialist II level may have statewide and enterprise-wide impacts. Consequences include lost funding, project failure, failed business strategy, poor customer service and performance, risk exposure, and loss of business continuity.

ADA Notice: For individuals with sensory disabilities, this document is available in alternate formats. For information, please call the EEO Officer at (916) 324-1541, email at eeo@hsr.ca.gov, or write to: California High-Speed Rail Authority, at 770 L Street, Suite 620, Sacramento, CA 95814.

Consequences also include error in making decisions or giving advice that would have a serious detrimental effect on the operating efficiency of the undertaking or function.

SPECIAL PERSONAL CHARACTERISTICS:

- Ability to learn new technologies quickly and thoroughly.
- Ability to resolve technical problems quickly and tactfully.
- Ability to read and interpret operating and maintenance instructions and procedure manuals.
- Ability to handle multiple projects simultaneously.
- Ability to work effectively under tight time constraints, client demands, and the pressure of multiple deadlines.

INTERPERSONAL SKILLS:

- Excellent communications skills.
- Excellent analytical skills to troubleshoot problems or offer alternatives for problem resolution.

WORK ENVIRONMENT:

Employee will work in a climate-controlled high-rise office building under artificial light. However, due to periodic problems with power, heating and air conditioning, the building temperature may fluctuate. Employee may be required to travel outside of their workstation to perform general tasks. The employee will also be required to:

- Work occasional overtime as necessary.
- Occasionally lift and/or move IT equipment weighing up to 30 pounds.
- Effectively work under stress.
- Occasionally travel as required.

I have read, and understand the duties listed above and can perform them either with or without reasonable accommodation. (If you believe you may require reasonable accommodation, please discuss this with your hiring supervisor. If you are unsure whether you require reasonable accommodation, inform the hiring supervisor who will discuss your concerns with the Reasonable Accommodation Coordinator.)

Name of Employee: ____

Signature:	Date:

ADA Notice: For individuals with sensory disabilities, this document is available in alternate formats. For information, please call the EEO Officer at (916) 324-1541, email at eeo@hsr.ca.gov, or write to: California High-Speed Rail Authority, at 770 L Street, Suite 620, Sacramento, CA 95814.

I have discussed the duties with and provided a copy of this duty statement to the employee named above.

Name of Supervisor____

Signature:	Date:

ADA Notice: For individuals with sensory disabilities, this document is available in alternate formats. For information, please call the EEO Officer at (916) 324-1541, email at eeo@hsr.ca.gov, or write to: California High-Speed Rail Authority, at 770 L Street, Suite 620, Sacramento, CA 95814.